RSAC 2025 Conference

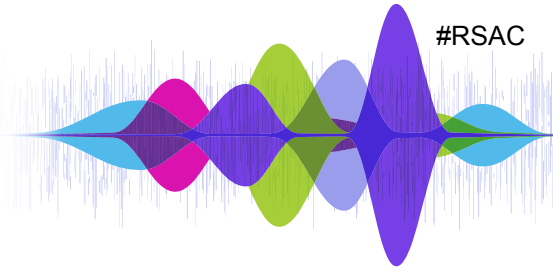
Many Voices.
One Community.

SESSION ID: CLS-T09

Critiquing Cloud Criminals: Ready For Smarter Cloud Attacks?

Nick Frichette

Staff Security Researcher
Datadog
https://www.linkedin.com/in/nick-frichette/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Nick Frichette

- Staff Security Researcher at Datadog
- Creator/maintainer of

Hacking the Cloud

@Frichette_n

@frichetten.com

Terrible

In This Talk

Look at a common threat actor technique

Data gathered from 56 real-world incidents

In This Talk

Look at a common threat actor technique

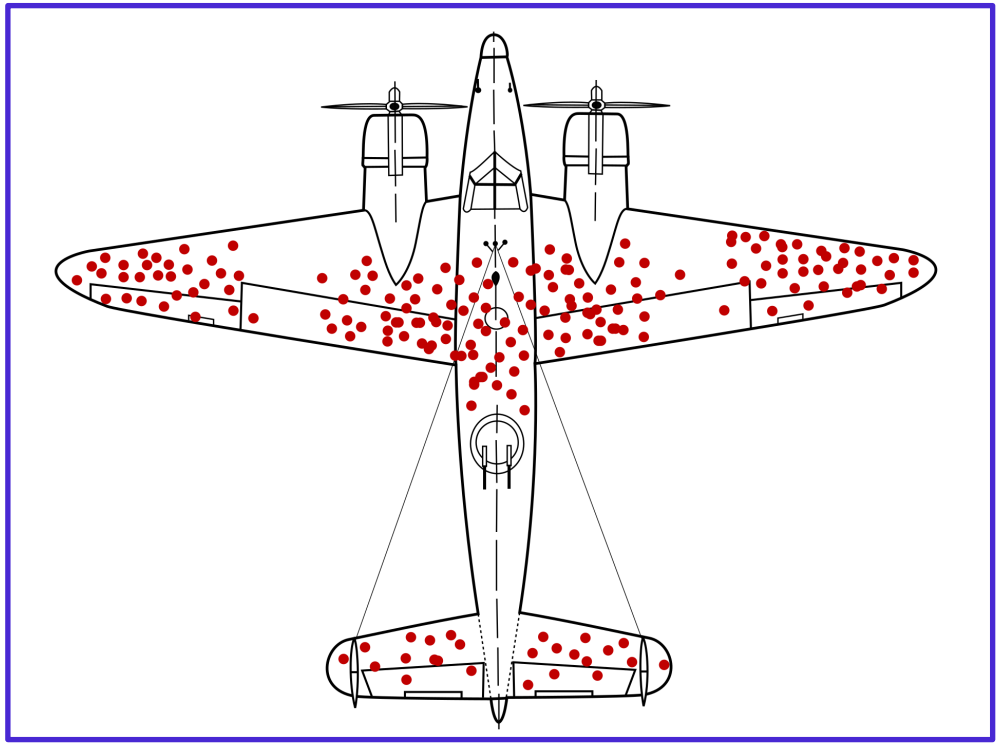
Talk about why it's terrible

In This Talk

Look at a common threat actor technique
Talk about why it's terrible
Demonstrate better techniques

A Few Disclaimers

- We are analyzing public incidents that got caught
  - Even with their terrible cloud skills, many of these incidents were successful
  - It shows how far we still have to go as an industry
- Public reports don't tell the whole story
- Selection bias!
- We are going to look at some techniques…you can't do anything about.

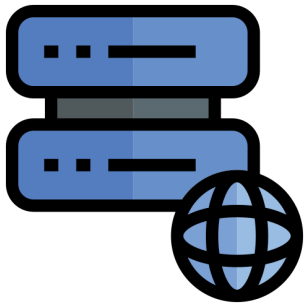


RSAC | 2025 Conference

How do you get initial access in AWS?

Many Voices.
One Community.

Initial Access in AWS



Exploit Internet Facing Compute

Insider Threat

Leaked Credentials

Social Engineering/ Compromise Dev/Admin

IAM Cross-Account Permissions

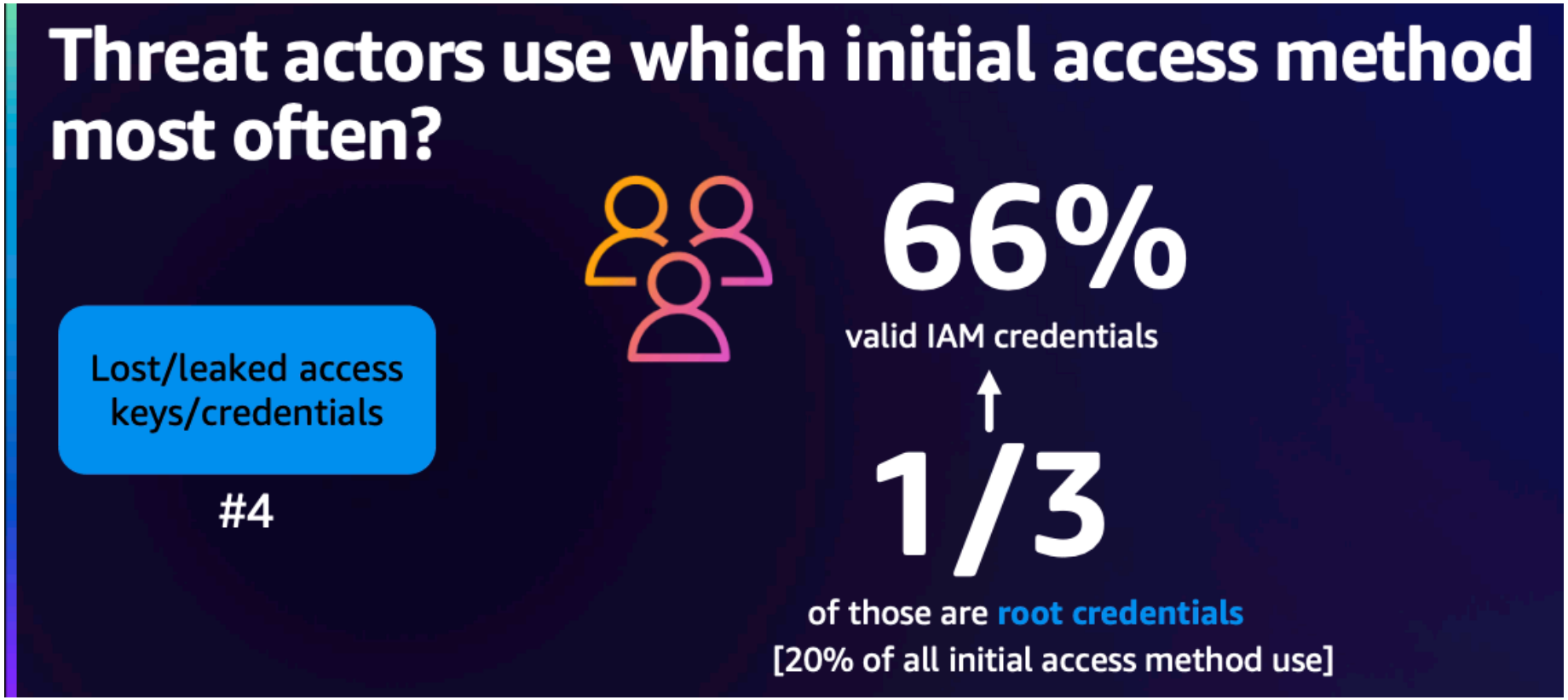
It all starts with some keys

- 66% of incidents started with exposed AWS Credentials

Leaked
Credentials

It all starts with some keys

- 66% of incidents started with exposed AWS Credentials



Source: https://reinforce.awsevents.com/content/dam/reinforce/2024/slides/TDR432_New-tactics-and-techniques-for-proactive-threat-detection.pdf

RSAC 2025 Conference

Using Those Keys

RSAC 2025 Conference

Using Those Keys (poorly)

CloudTrail: Cloud Hacking's Buzzkill

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
    },
    "eventTime": "2025-03-19T18:31:27Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "GetCallerIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "2.2.2.2",
    "userAgent": "aws-cli/2.22.12 md/awscrt#0.22.0 ua/2.0 os/macos#24.3.0 md/arch#arm64
lang/python#3.12.7 md/pyimpl#CPython md/command#sts.get-caller-identity",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management"
}
```


Note: Truncated for space

CloudTrail: Cloud Hacking's Buzzkill

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
    },
    "eventTime": "2025-03-19T18:31:27Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "GetCallerIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "2.2.2.2",
    "userAgent": "aws-cli/2.22.12 md/awscrt#0.22.0 ua/2.0 os/macos#24.3.0 md/arch#arm64
lang/python#3.12.7 md/pyimpl#CPython md/command#sts.get-caller-identity",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management"
}
```


Note: Truncated for space

CloudTrail: Cloud Hacking's Buzzkill

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
    },
    "eventTime": "2025-03-19T18:31:27Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "GetCallerIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "2.2.2.2",
    "userAgent": "aws-cli/2.22.12 md/awscrt#0.22.0 ua/2.0 os/macos#24.3.0 md/arch#arm64
lang/python#3.12.7 md/pyimpl#CPython md/command#sts.get-caller-identity",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management"
}
```


Note: Truncated for space

CloudTrail: Cloud Hacking's Buzzkill

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
    },
    "eventTime": "2025-03-19T18:31:27Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "GetCallerIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "2.2.2.2",
    "userAgent": "aws-cli/2.22.12 md/awscrt#0.22.0 ua/2.0 os/macos#24.3.0 md/arch#arm64
lang/python#3.12.7 md/pyimpl#CPython md/command#sts.get-caller-identity",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management"
}
```


Note: Truncated for space

CloudTrail: Cloud Hacking's Buzzkill

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
    },
    "eventTime": "2025-03-19T18:31:27Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "GetCallerIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "2.2.2.2",
    "userAgent": "aws-cli/2.22.12 md/awscrt#0.22.0 ua/2.0 os/macos#24.3.0 md/arch#arm64
lang/python#3.12.7 md/pyimpl#CPython md/command#sts.get-caller-identity",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management"
}
```


Note: Truncated for space

CloudTrail: Cloud Hacking's Buzzkill

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
    },
    "eventTime": "2025-03-19T18:31:27Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "GetCallerIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "2.2.2.2",
    "userAgent": "aws-cli/2.22.12 md/awscrt#0.22.0 ua/2.0 os/macos#24.3.0 md/arch#arm64
lang/python#3.12.7 md/pyimpl#CPython md/command#sts.get-caller-identity",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management"
}
```


Note: Truncated for space

The User Agent is a Snitch

aws-cli/1.19.59 Python/3.9.2 Linux/5.10.0-kali5-amd64 botocore/1.27.43	UA associated with aws_consoler used by the adversary

PenTest:IAMUser/KaliLinux

An API was invoked from a Kali Linux machine.

Default severity: Medium

- **Data source:** CloudTrail management event

This finding informs you that a machine running Kali Linux is making API calls using credentials that belong to the listed AWS account in your environment. Kali Linux is a popular penetration testing tool that security professionals use to identify weaknesses in EC2 instances that require patching. Attackers also use this tool to find EC2 configuration weaknesses and gain unauthorized access to your AWS environment.

Remediation recommendations:

If this activity is unexpected, your credentials may be compromised. For more information, see Remediating potentially compromised AWS credentials.

The User Agent is a Snitch

aws-cli/1.19.59 Python/3.9.2 Linux/5.10.0-kali5-amd64 botocore/1.27.43	UA associated with aws_consoler used by the adversary

PenTest:IAMUser/KaliLinux

An API was invoked from a Kali Linux machine.

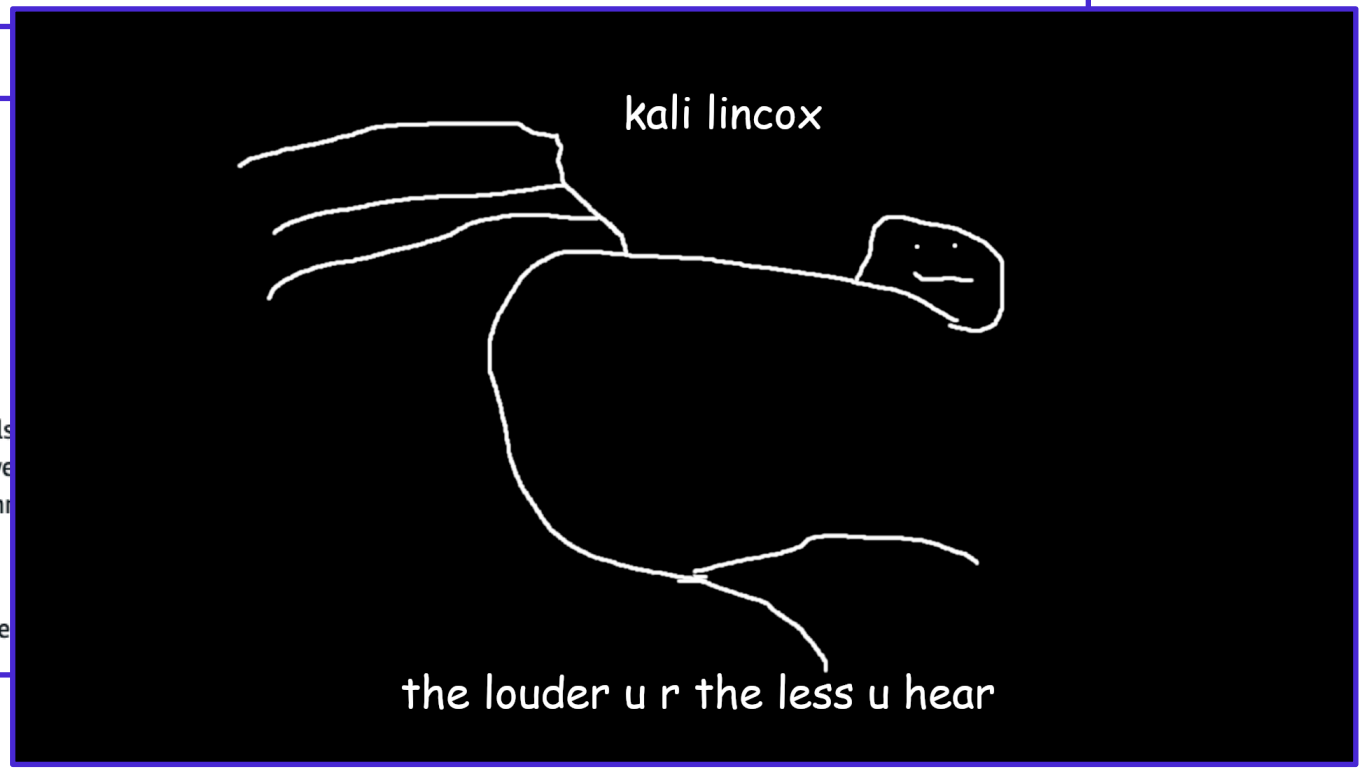
Default severity: Medium

- **Data source:** CloudTrail management event

This finding informs you that a machine running Kali Linux is making API calls
popular penetration testing tool that security professionals use to identify we
configuration weaknesses and gain unauthorized access to your AWS environ

Remediation recommendations:

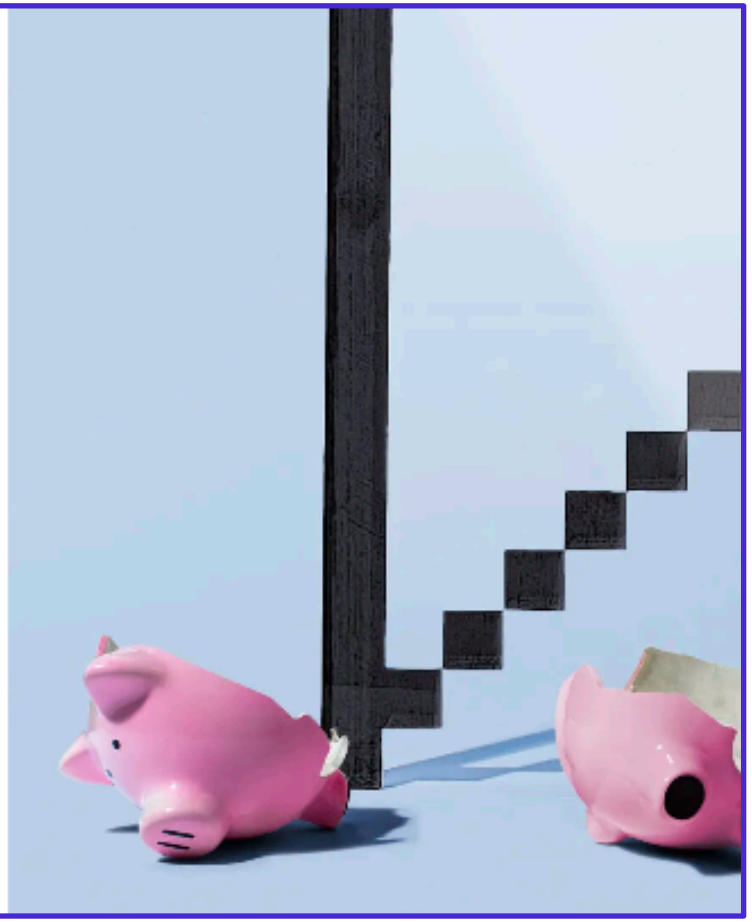
If this activity is unexpected, your credentials may be compromised. For more



The $1.5 Billion Bybit Hack

How the Biggest Crypto Heist in History Went Down

The cryptocurrency exchange Bybit lost $1.5 billion to North Korean hackers last month — and it all traced back to an account on a free digital storage service.



Source: https://www.nytimes.com/2025/03/06/technology/bybit-crypto-hack-north-korea.html

The $1.5 Billion Bybit Hack

identified on Developer1's workstation.

- The attacker use of Developer1's AWS account originated from ExpressVPN IP addresses with User-Agent strings containing `distrib#kali.2024`. Mandiant assesses that this User-Agent string indicates use of Kali Linux which is designed for offensive security practitioners. Mandiant has previously observed UNC4899 using ExpressVPN infrastructure and Kali when conducting their operations.
- Safe{Wallet}'s AWS configuration required MFA re-authentication for Security Token Service (STS) sessions

Source: https://x.com/safe/article/1897663514975649938/media/1897649329432645632

The $1.5 Billion Bybit Hack

PRELIMINARY INVESTIGATION REPORT | Safe{Wallet}

- Analysis of the subsequent network traffic indicates that UNC4899 utilized the open-source offensive framework MythicAgents. Mandiant has observed UNC4899 using Mythic Poseidon, a Golang agent targeting macOS and Linux, in previous attacks.
- The malicious AWS activity identified to date spans from February 5, 2025 to February 21, 2025 using Developer1's AWS session tokens. Analysis of attacker activity during this timeframe is ongoing.

Source: https://x.com/safe/article/1897663514975649938/media/1897649381634973696

It affects tools too!

IAN AHL | 22 MAY 2023 BACK TO BLOGS

UNMASKING GUI-VIL: FINANCIALLY MOTIVATED CLOUD THREAT ACTOR

```
{
        "eventVersion": "1.08",
        "userIdentity": {
                "type": "IAMUser",
                "principalId": "redacted",
                "arn": "arn:aws:iam::redacted:user/terraform",
                "accountId": "redacted",
                "accessKeyId": "AKIA****",
                "userName": "terraform"
        },
        "eventTime": "2023-04-18T15:27:22.0000000Z",
        "eventSource": "iam.amazonaws.com",
        "eventName": "GetLoginProfile",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "36.85.110.142",
        "userAgent": "S3 Browser 9.5.5 <https://s3browser.com>",
        "requestParameters": {
                "userName": "andy"
        },
        "responseElements": null
```


Source: https://permiso.io/blog/s/unmasking-guivil-new-cloud-threat-actor/

It affects tools too!

Maintain Presence (IAM)

In order to maintain a presence in the victim organization, GUI-vil has leveraged several different mechanisms. Based on observed activity, they exclusively utilize S3 Browser to make creations and modifications to the `IAM` service.

It affects tools too!

Maintain Presence (

In order to maintain a presence in the vict
leveraged several different mechanisms.
they exclusively utilize S3 Browser to make creations and modifications
to the `IAM` service.

It is rampant!

Trouble in Paradise

July 6, 2021 by darklabhk

IAN AHL | 20 JUN 2022

ANATOMY OF AN ATTACK: EXPOSED KEYS TO CRYPTO MINING

CLOUD CYBERSECURITY RESEARCH

Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments

CLOUD CYBERSECURITY RESEARCH

When a Zero Day and Access Keys Collide in the Cloud: Responding to the SugarCRM Zero-Day Vulnerability

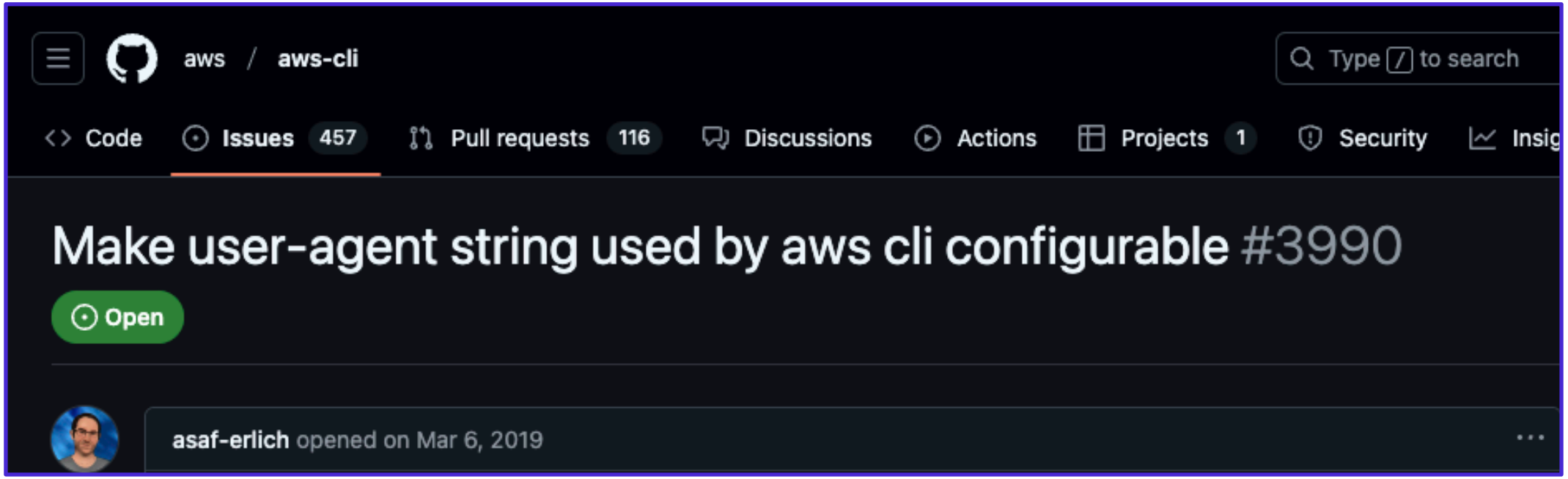
DATADOG

How do we avoid this? It's easy!

- User agent strings are 100% attacker controlled
- You can appear to be whatever kind of machine you want
- If using the AWS SDK, this value is 100% configurable

How do we avoid this? It's easy!

- User agent strings are 100% attacker controlled
- You can appear to be whatever kind of machine you want
- If using the AWS SDK, this value is 100% configurable



Burp Suite match and replace

Tools › Proxy

HTTP match and replace rules

Use these settings to automatically replace parts of HTTP requests and responses passing through the Proxy.

☐ Only apply to in-scope items

Add | Edit | Remove | Up | Down

Enabled	Item	Match	Replace	Type	Comment
☐	Request header	^User-Agent.*$	User-Agent: Mozilla/4.0 (com...	Regex	Emulate IE
☐	Request header	^User-Agent.*$	User-Agent: Mozilla/5.0 (iPho...	Regex	Emulate iOS
☐	Request header	^User-Agent.*$	User-Agent: Mozilla/5.0 (Linux...	Regex	Emulate Android
☐	Request header	^If-Modified-Since.*$		Regex	Require non-cached respo...
☐	Request header	^If-None-Match.*$		Regex	Require non-cached respo...
☐	Request header	^Referer.*$		Regex	Hide Referer header
☐	Request header	^Accept-Encoding.*$		Regex	Require non-compressed r...

Burp Suite match and replace

RSAC | 2025 Conference

How do they know if the keys work?

Many Voices.
One Community.

How do they know the keys work?

GetCallerIdentity

PDF

Returns details about the IAM user or role whose credentials are used to call the operation.

```
nick.frichette@host ~ % aws sts get-caller-identity
{
    "UserId": "AROA123ABC456DEF789GH:nick.frichette@example.com",
    "Account": "111111111111",
    "Arn": "arn:aws:sts::111111111111:assumed-role/admin-role/nick.frichette@example.com"
}
```

sts:GetCallerIdentity in the Wild

DATADOG Security Labs

ARTICLES CLOUD SECURITY A

RESEARCH

Tales from the cloud trenches: Using AWS CloudTrail to identify malicious activity and spot phishing campaigns

March 15, 2024

AWS THREAT DETECTION

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

NICKOLAS SHARP,

Defendant.

CLOUD CYBERSECURITY RESEARCH

When a Zero Day and Access Keys Collide in the Cloud: Responding to the SugarCRM Zero-Day Vulnerability

13 min read

sts:GetCalle

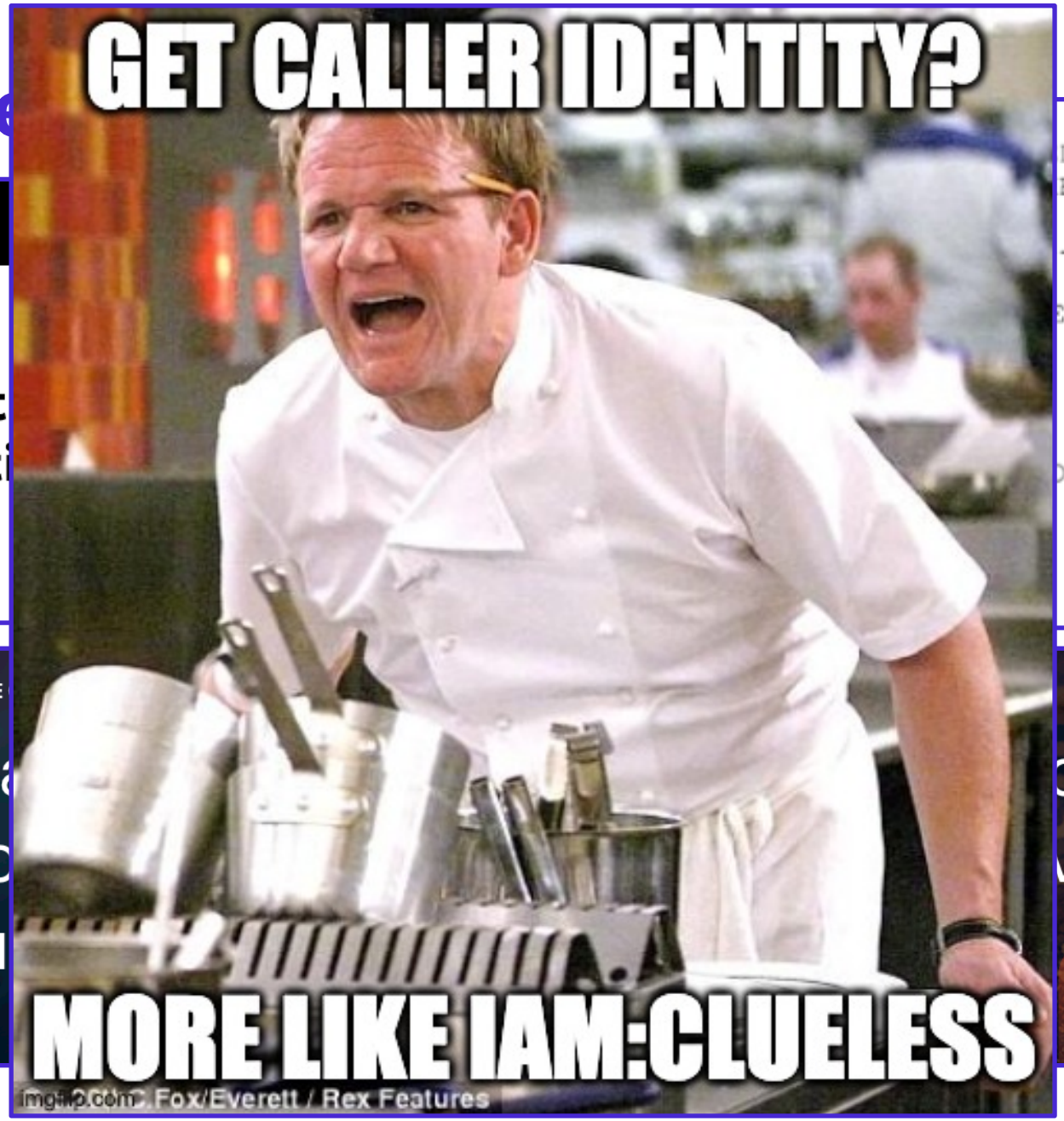
DATADOG Security Labs

RESEARCH

Tales from the cloud t
identify malicious acti

March 15, 2024

AWS THREAT DETECTION



D STATES DISTRICT COURT
ERN DISTRICT OF NEW YORK

ED STATES OF AMERICA

- v. -

OLAS SHARP,

Defendant.

CLOUD CYBERSE

When a
the Clo
Day Vu

13 min read

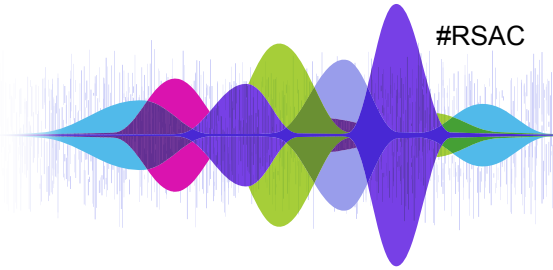
de in
M Zero-

CloudTrail: It's Still a Buzzkill

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
    },
    "eventTime": "2025-03-19T18:31:27Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "GetCallerIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "2.2.2.2",
    "userAgent": "aws-cli/2.22.12 md/awscrt#0.22.0 ua/2.0 os/macos#24.3.0 md/arch#arm64
lang/python#3.12.7 md/pyimpl#CPython md/command#sts.get-caller-identity",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management"
}
```


Note: Truncated for space

Use an API that Doesn’t Log to CloudTrail



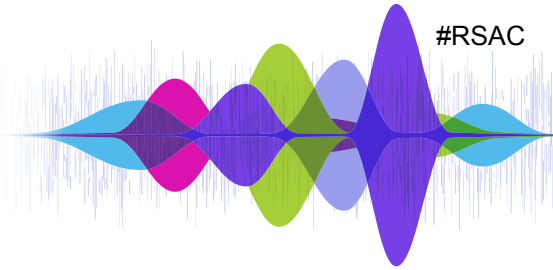
Use an API that Doesn't Log to CloudTrail

```
nick.frichette@host ~ % aws sqs list-queues

An error occurred (AccessDenied) when calling the ListQueues operation: User:
arn:aws:sts::111111111111:assumed-role/noperm/noperm is not authorized to perform:
sqs:listqueues on resource: arn:aws:sqs:us-east-1:111111111111: because no identity-
based policy allows the sqs:listqueues action
```

```
nick.frichette@host ~ % aws sts get-caller-identity
{
    "UserId": "AROA123ABC456DEF789GH:nick.frichette@example.com",
    "Account": "111111111111",
    "Arn": "arn:aws:sts::111111111111:assumed-role/admin-role/nick.frichette@example.com"
}
```

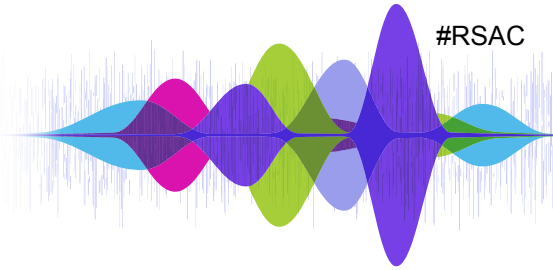
Use an API that Doesn’t Log to CloudTrail



```
nick.frichette@host ~ % aws sqs list-queues

An error occurred (InvalidClientTokenId) when calling the ListQueues operation: The
security token included in the request is invalid.
```

Use an API that Doesn't Log to CloudTrail



```
nick.frichette@host ~ % aws pinpoint-sms-voice send-voice-message

An error occurred (AccessDeniedException) when calling the SendVoiceMessage operation:
User: arn:aws:sts::111111111111:assumed-role/noperm/noperm is not authorized to perform:
sms-voice:SendVoiceMessage on resource: arn:aws:sms-voice:us-east-
1:111111111111:/v1/sms-voice/voice/message
```

The following Amazon Pinpoint SMS and Voice version 1 API action **isn't** logged in CloudTrail:

- SendVoiceMessage

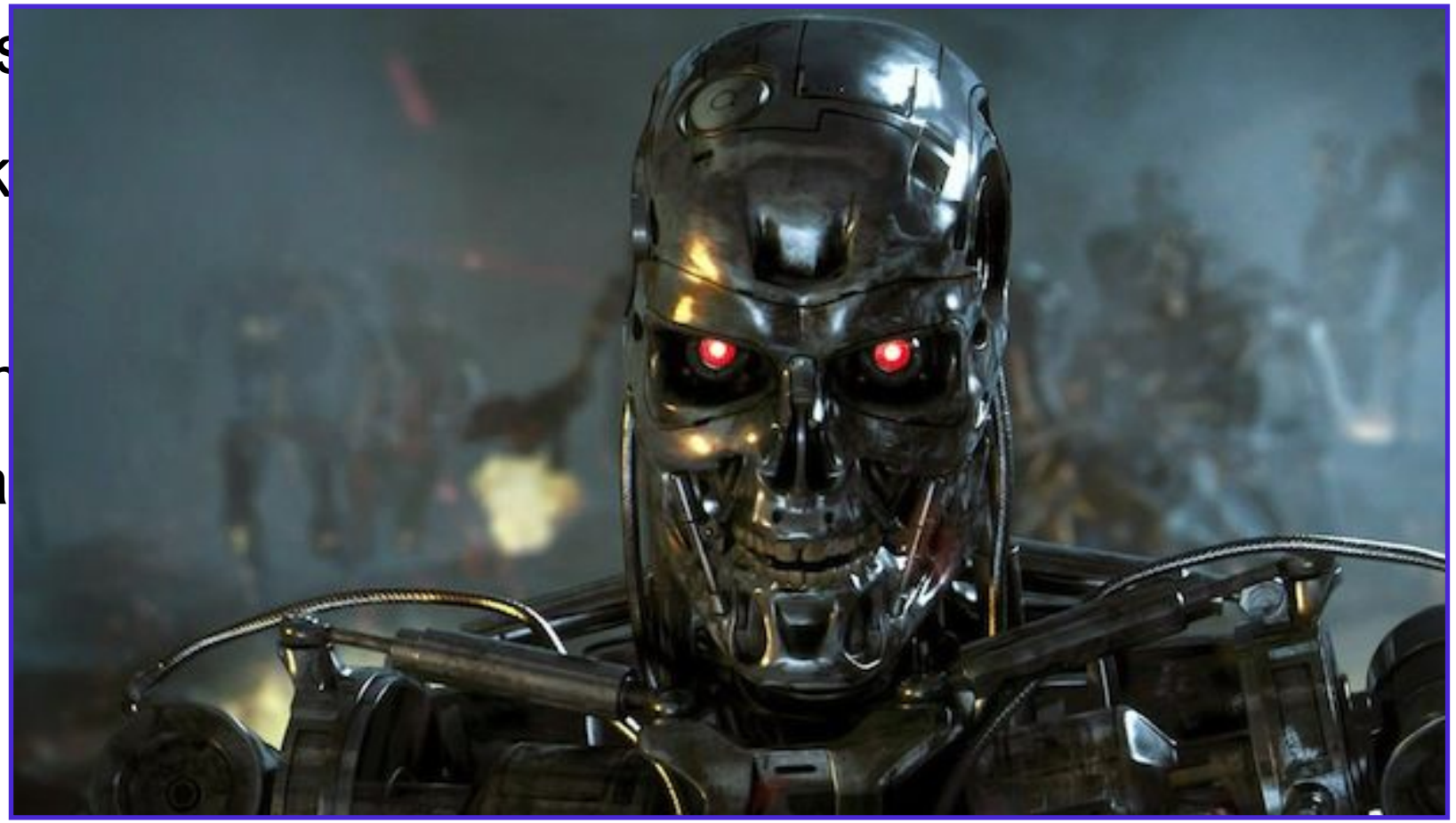
Source: https://docs.aws.amazon.com/pinpoint/latest/developerguide/pinpoint-sms-voice-cloudtrail-actions.html

sts:GetCallerIdentity generates logs you don't need

- 0 logs is better (for attackers) than 1
- Worth knowing some services legitimately use this behavior
  - EKS
  - Pulumi
  - Humans
- We are looking for anomalies

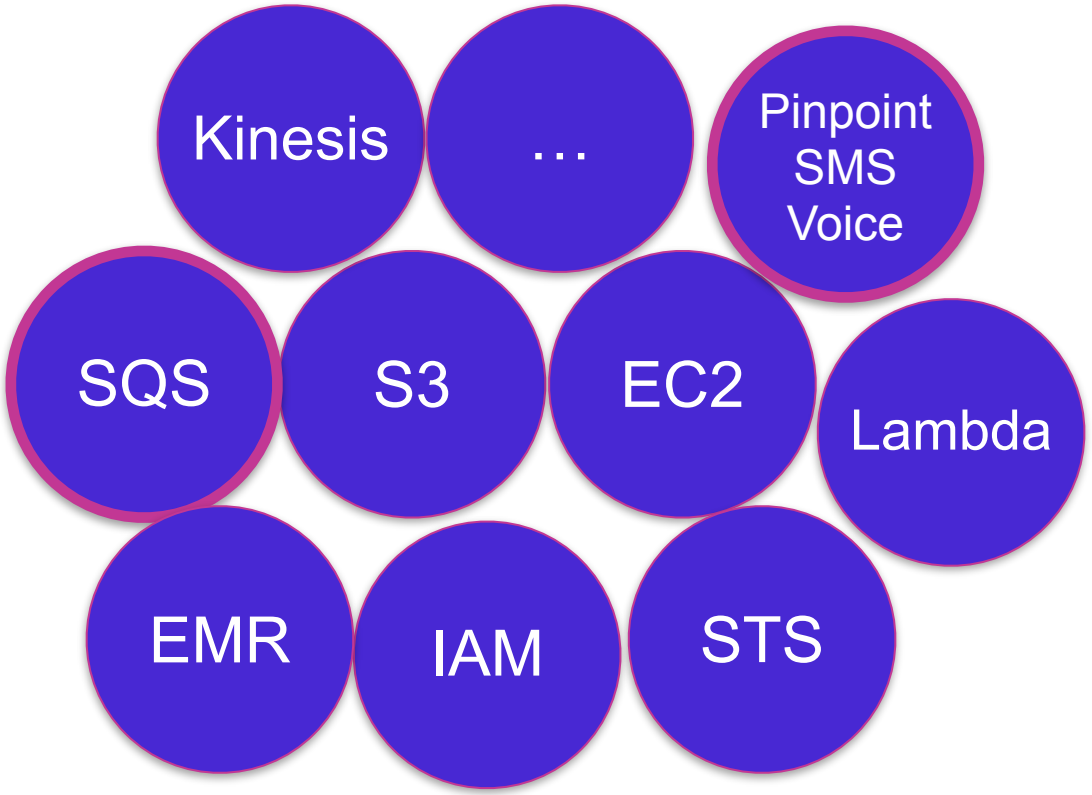
sts:GetCallerIdentity generates logs you don't need

- 0 logs is
- Worth k havior
  - EKS
  - Pulum
  - Huma
- We are

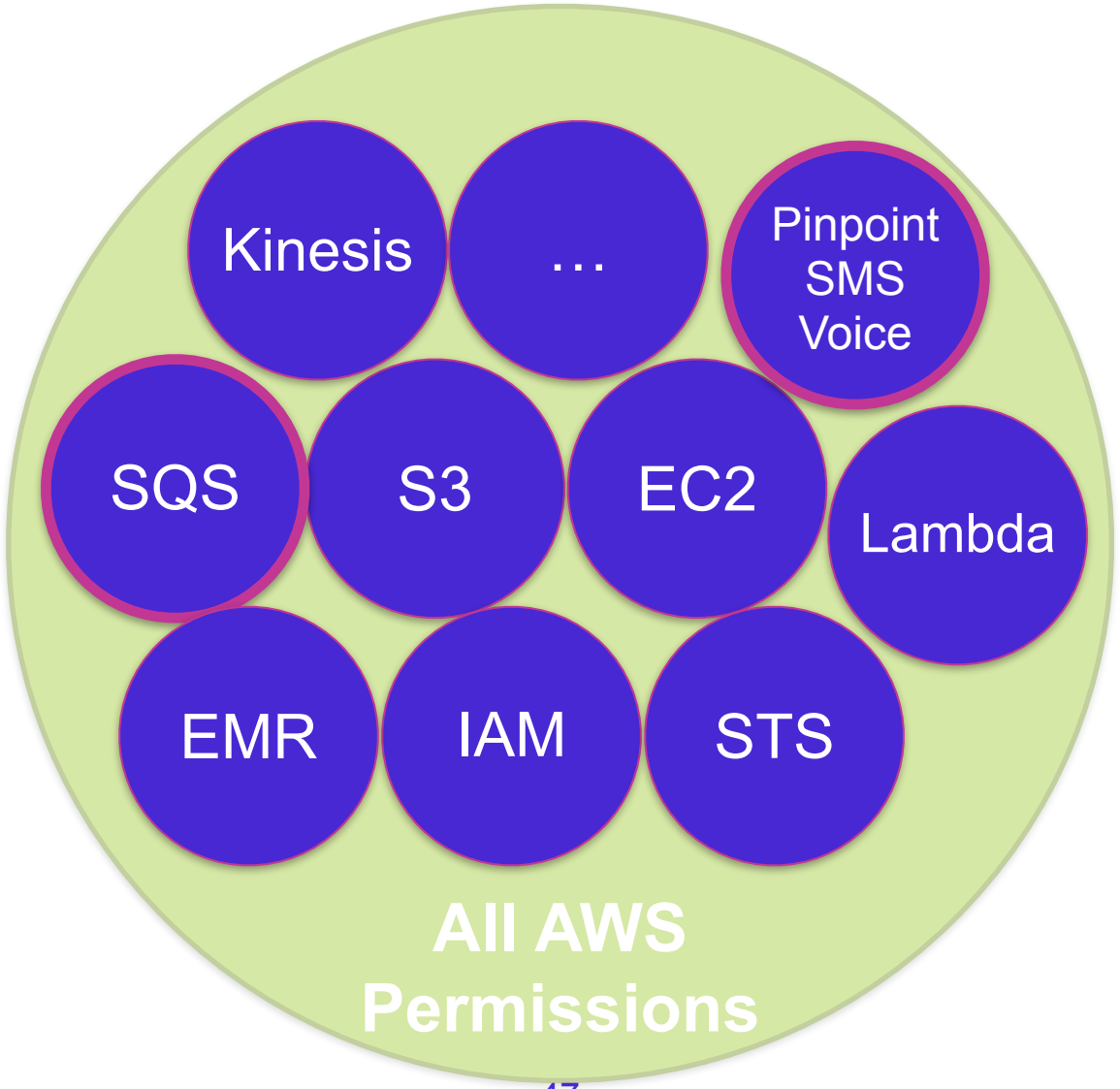


But what if the keys DO have privileges?

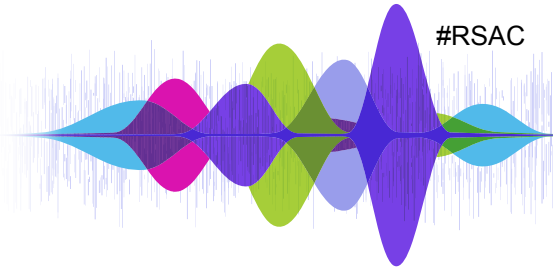
But what if the keys DO have privileges?



But what if the keys DO have privileges?



But what if the keys DO have privileges?



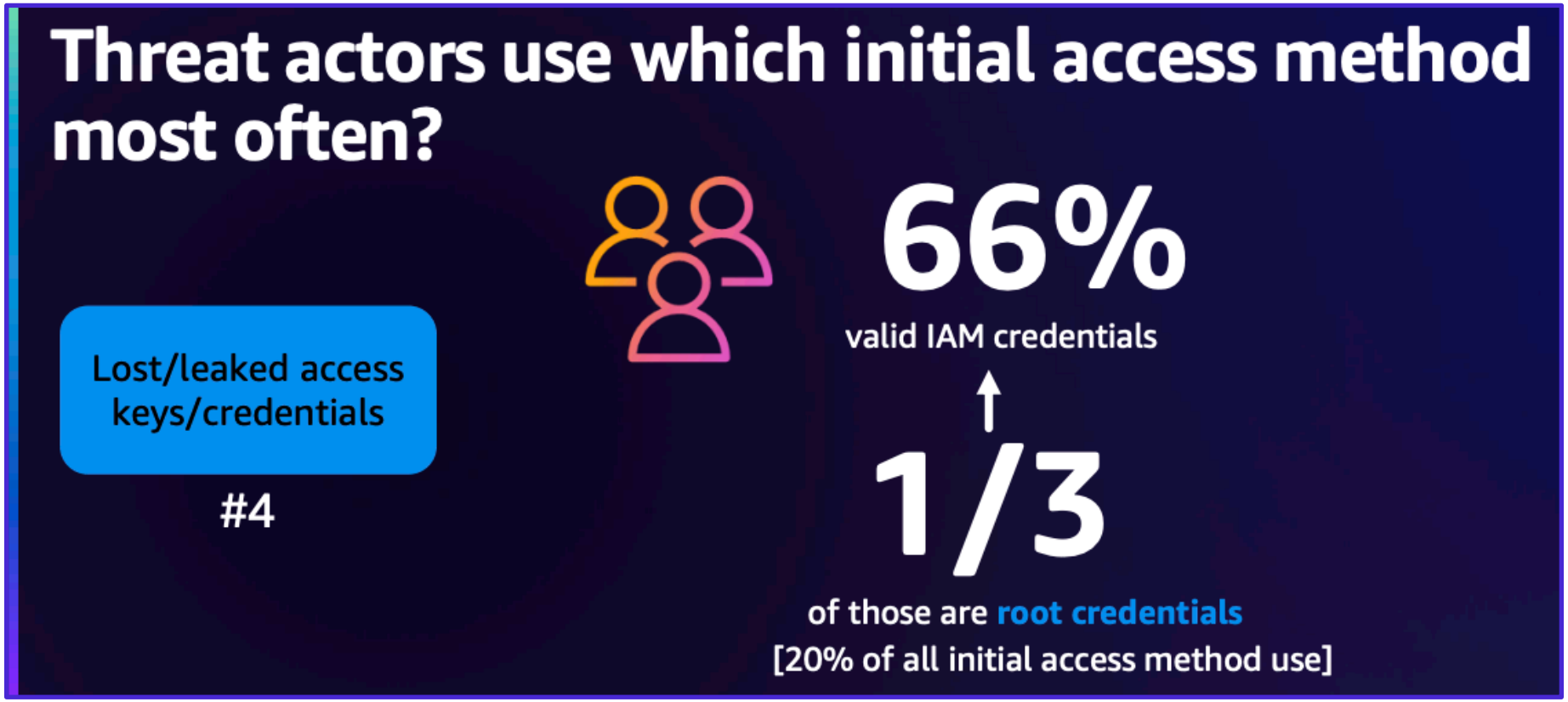
```
nick.frichette@host:~$ aws sts get-access-key-info --access-key-id=AKIA1234567890123456
{
    "Account": "123456789012"
}
```

RSAC | 2025 Conference

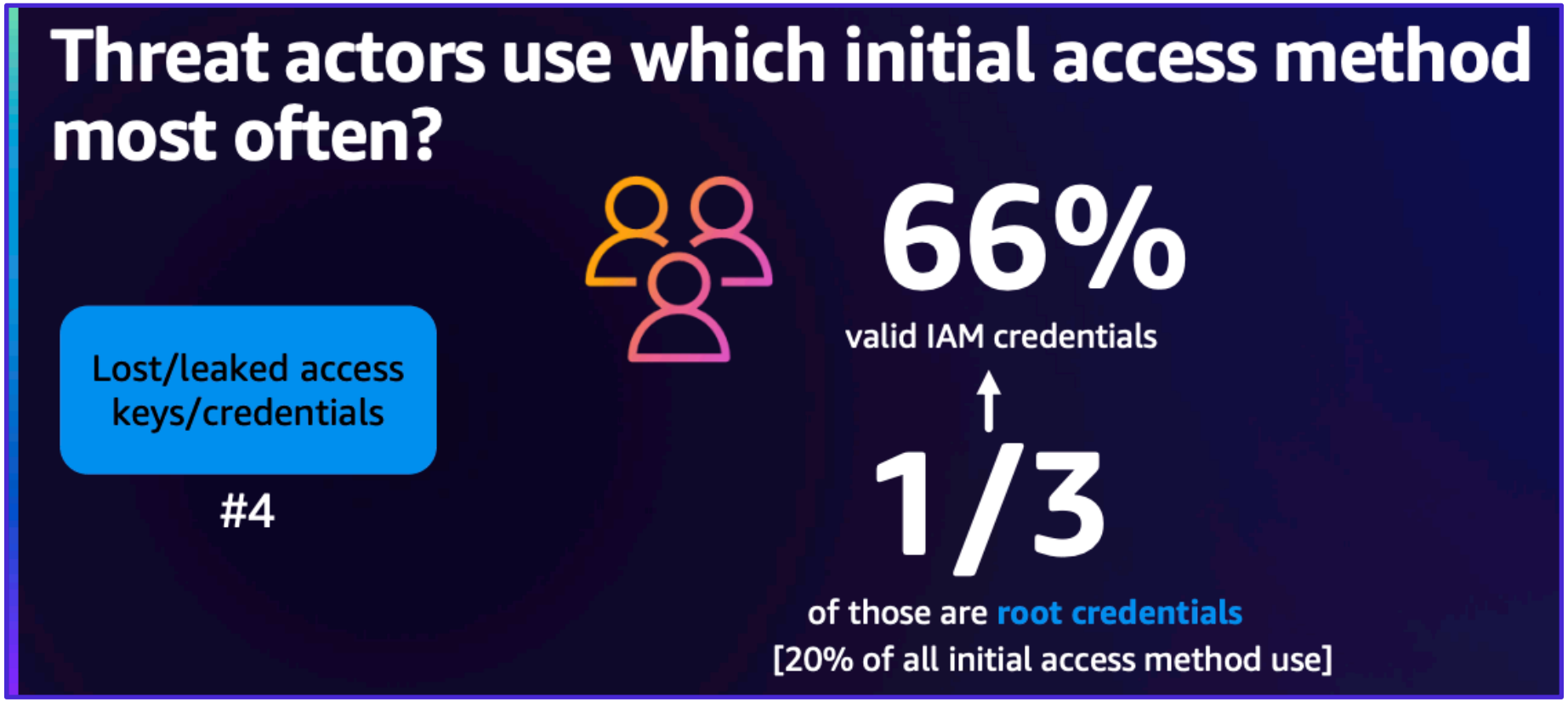
Enumeration Time

Many Voices.
One Community.

What access do I have?



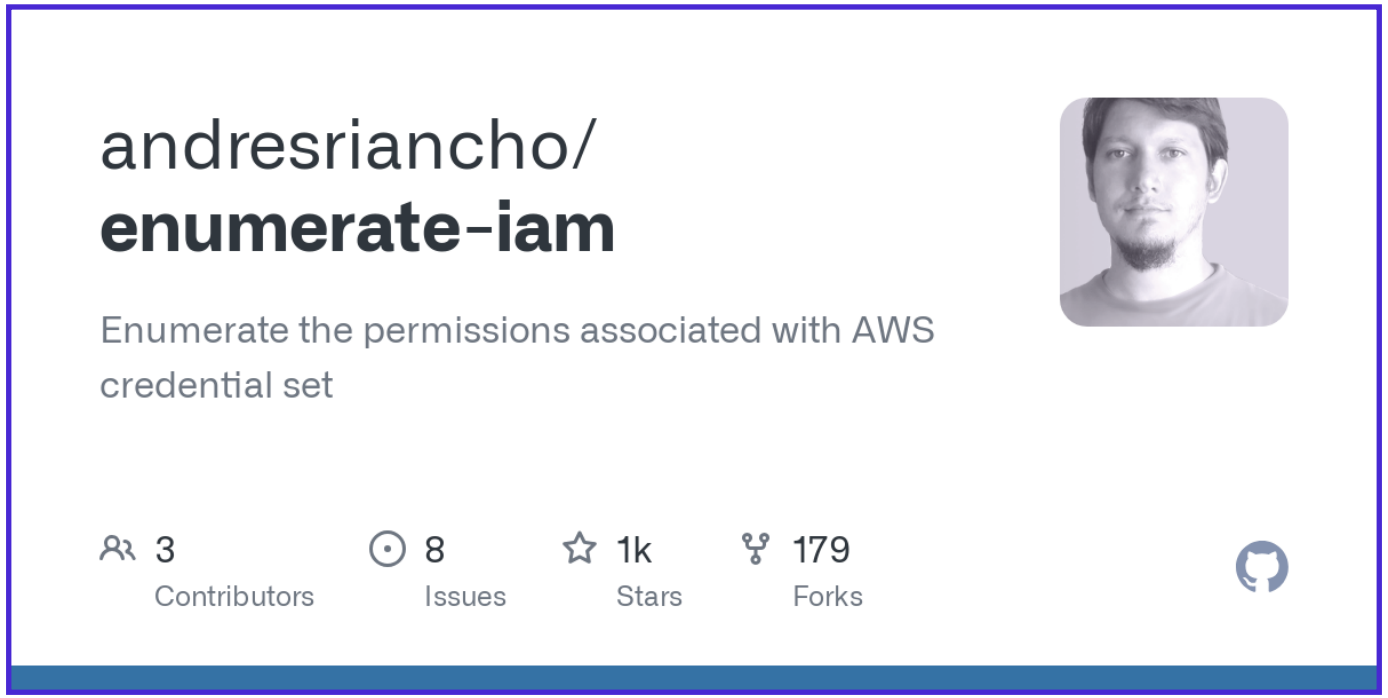
What access do I have?



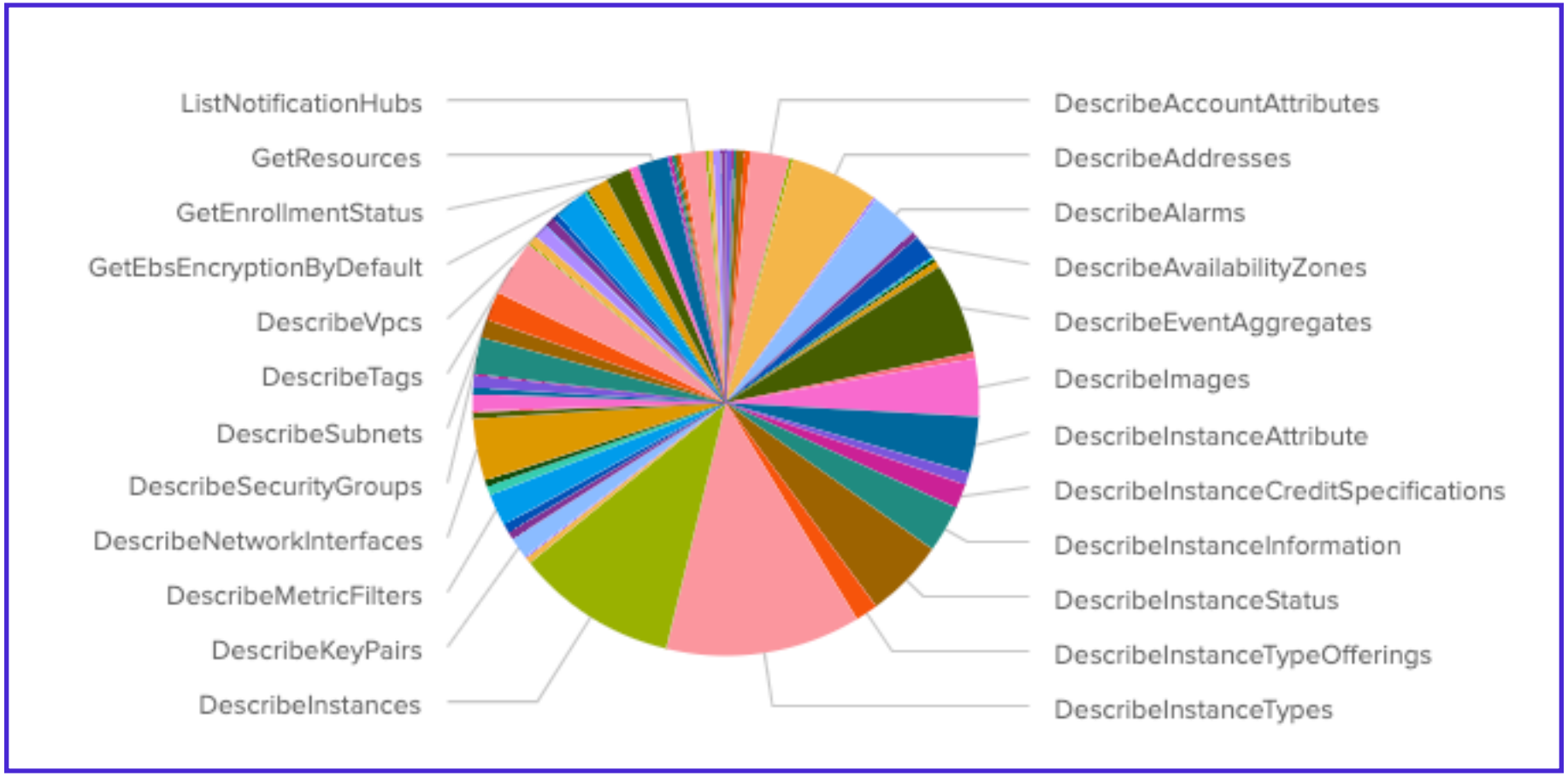
43% of leaked credentials had administrative privileges!

What access do I have?

- Traditionally, this is achieved through some kind of brute force

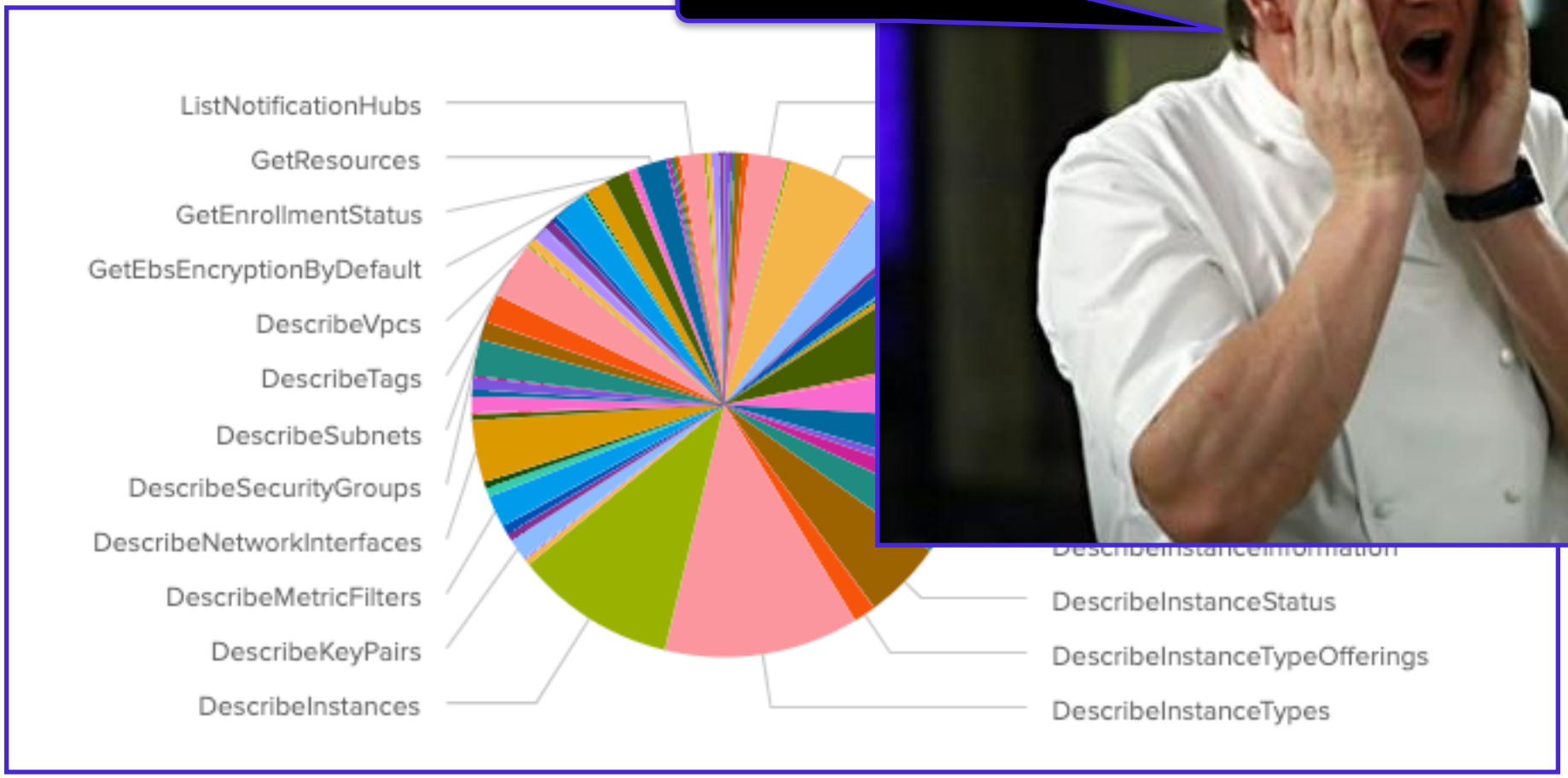


Noisy Enumeration 😬



Source: https://www.invictus-ir.com/news/the-curious-case-of-dangerdev-protonmail-me

Noisy Enumeration 😬



Source: https://www.invictus-ir.com/news/the-curious-case-of-dangerdev-protonmail-me

Key Services Attackers Target (and Enumerate)

- SES/SNS - Spam/Phishing
- EC2/ECS - Crypto mining
- IAM - Persistence/Priv Esc
- S3 - Looking for goodies

Option 1: CloudTrail Bypass

- Two tiers of bypass:
  - Full - Perform an action that doesn't get logged to CloudTrail
    - This is the most severe kind
    - AWS considers this a vulnerability

RESEARCH

AWS CloudTrail vulnerability: Undocumented API allows CloudTrail bypass

January 17, 2023

AWS VULNERABILITY DISCLOSURE

RESEARCH

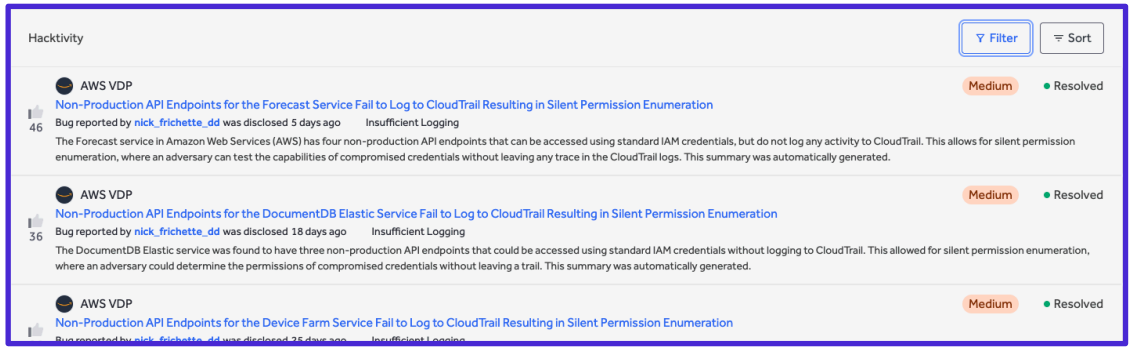
Bypassing CloudTrail in AWS Service Catalog, and Other Logging Research

March 20, 2023

AWS VULNERABILITY DISCLOSURE

Option 1: CloudTrail Bypass

- Two tiers of bypass:
  - Full - Perform an action that doesn't get logged to CloudTrail
    - This is the most severe kind
    - AWS considers this a vulnerability
  - Enumerative - Enumerates permissions but does not return results
    - Less severe
    - AWS also considers this a vulnerability


Hacktivity
Filter
Sort
AWS VDP
Medium
Resolved
Non-Production API Endpoints for the Forecast Service Fail to Log to CloudTrail Resulting in Silent Permission Enumeration
Bug reported by nick_frichette_dd was disclosed 5 days ago
Insufficient Logging
The Forecast service in Amazon Web Services (AWS) has four non-production API endpoints that can be accessed using standard IAM credentials, but do not log any activity to CloudTrail. This allows for silent permission enumeration, where an adversary can test the capabilities of compromised credentials without leaving any trace in the CloudTrail logs. This summary was automatically generated.
AWS VDP
Medium
Resolved
Non-Production API Endpoints for the DocumentDB Elastic Service Fail to Log to CloudTrail Resulting in Silent Permission Enumeration
Bug reported by nick_frichette_dd was disclosed 18 days ago
Insufficient Logging
The DocumentDB Elastic service was found to have three non-production API endpoints that could be accessed using standard IAM credentials without logging to CloudTrail. This allowed for silent permission enumeration, where an adversary could determine the permissions of compromised credentials without leaving a trail. This summary was automatically generated.
AWS VDP
Medium
Resolved
Non-Production API Endpoints for the Device Farm Service Fail to Log to CloudTrail Resulting in Silent Permission Enumeration

Option 2: iam:SimulatePrincipalPolicy

```
nick.frichette@host ~ % aws iam simulate-principal-policy \
--policy-source-arn arn:aws:iam::111111111111:user/SomeGuy \
--action-names "ec2:DescribeVPCs" "iam:ListUsers" "secretsmanager:ListSecrets"
{
    "EvaluationResults": [
        {
            "EvalActionName": "ec2:DescribeVPCs",
            "EvalDecision": "allowed"
        },
        {
            "EvalActionName": "iam:ListUsers",
            "EvalDecision": "implicitDeny"
        },
        {
            "EvalActionName": "secretsmanager:ListSecrets",
            "EvalDecision": "implicitDeny"
        }
    ]
}
```

Note: Truncated for space

Option 3: Resource Explorer

```
nick.frichette@host site % aws resource-explorer-2 list-resources
{
    "Resources": [
        {
            "Arn": "arn:aws:s3:::storage-bucket-dev",
            "LastReportedAt": "2025-03-25T01:27:17+00:00",
            "OwningAccountId": "111111111111",
            "Region": "us-east-1",
            "ResourceType": "s3:bucket",
        }
        {
            "Arn": "arn:aws:iam::111111111111:role/account-admin",
            "LastReportedAt": "2025-03-24T09:44:43+00:00",
            "OwningAccountId": "111111111111",
            "ResourceType": "iam:role",
        },
        {
            "Arn": "arn:aws:iam::111111111111:role/cool-role",
            "LastReportedAt": "2025-03-24T09:44:48+00:00",
            "OwningAccountId": "111111111111",
            "ResourceType": "iam:role",
        }
}
```

Note: Truncated for space

Option 3: Resource Explorer

```
nick.frichette@host site % aws resource-explorer-2 list-resources
{
    "Resources": [
        {
            "Arn": "arn:aws:s3:::s
            "LastReportedAt": "202
            "OwningAccountId": "11
            "Region": "us-east-1",
            "ResourceType": "s3:bu
        }
        {
            "Arn": "arn:aws:iam::1
            "LastReportedAt": "202
            "OwningAccountId": "11
            "ResourceType": "iam:r
        },
        {
            "Arn": "arn:aws:iam::1
            "LastReportedAt": "202
            "OwningAccountId": "11
            "ResourceType": "iam:rol
        }
}
```

Note: Truncated for space

RSAC | 2025 Conference

That's Too Hard. I Wanna use the Console

The AWS Console

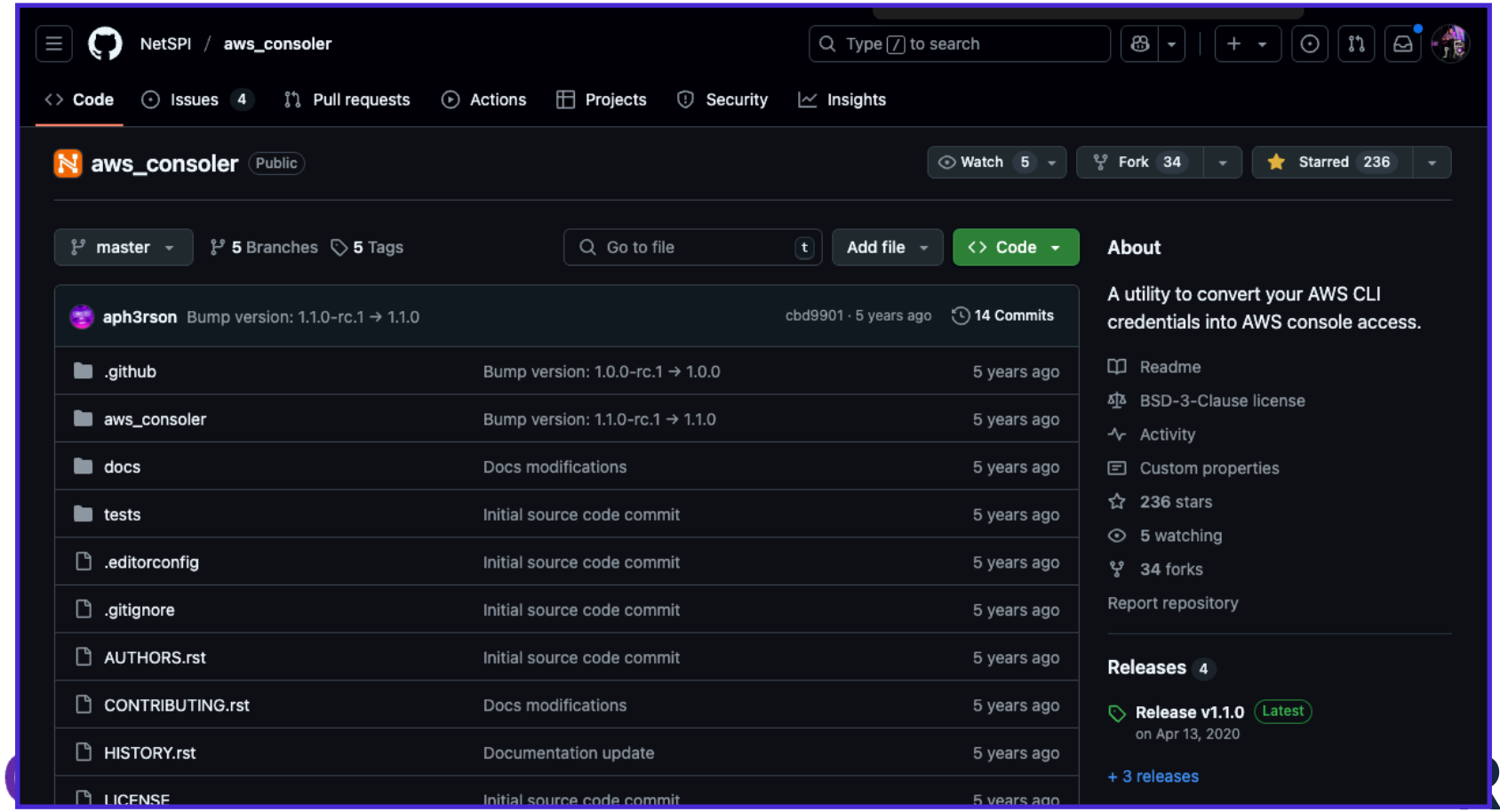
- The web portal for AWS infrastructure (ClickOps)
- Was involved in 21% of cases in our dataset.

The AWS Console

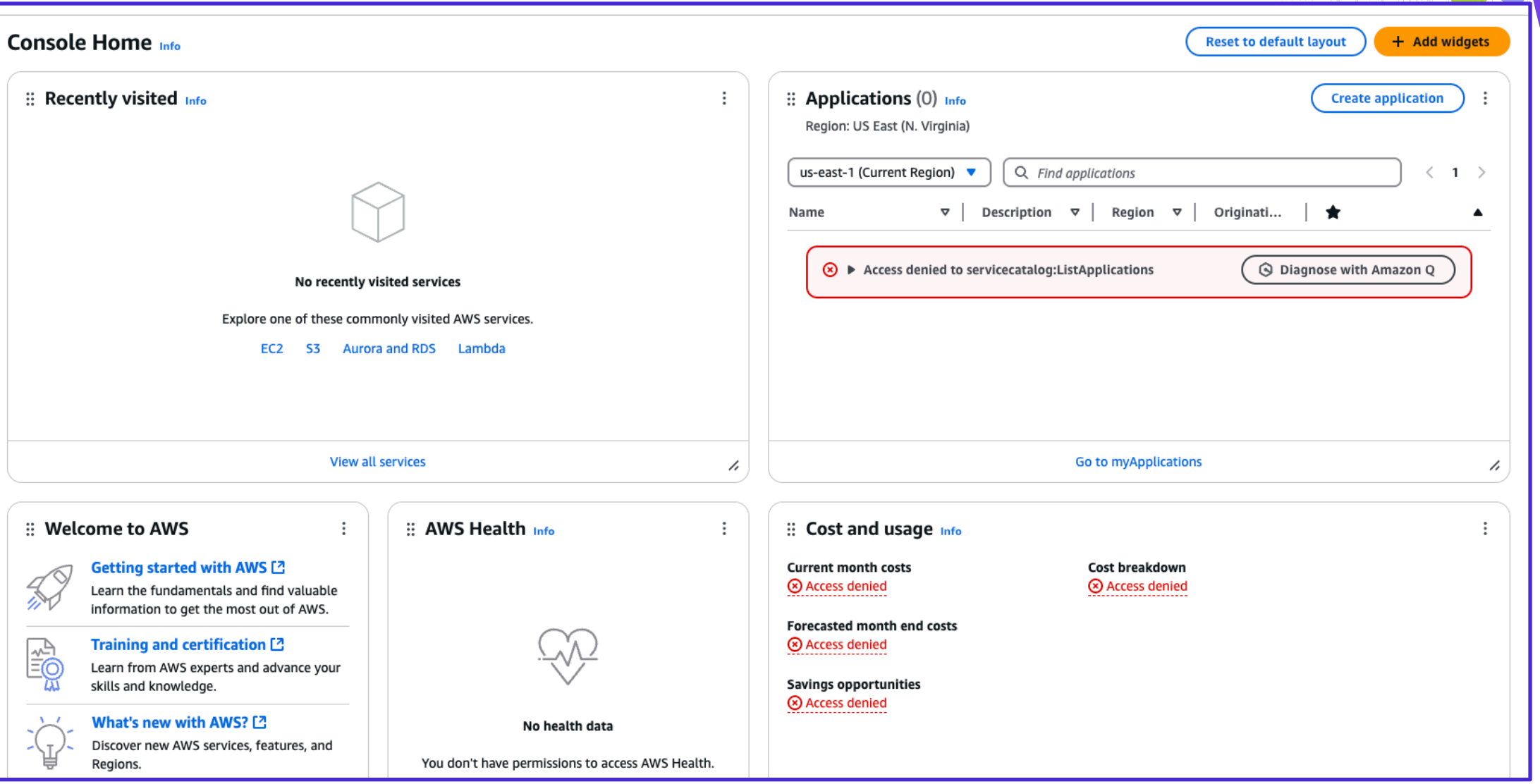
- The web portal for AWS infrastructure (ClickOps)
- Was involved in 21% of cases in our dataset.

aws_consoler

- Both long-lived (AKIA) and temporary (ASIA) access key's can generate console sign in links.



The AWS Console is Loud

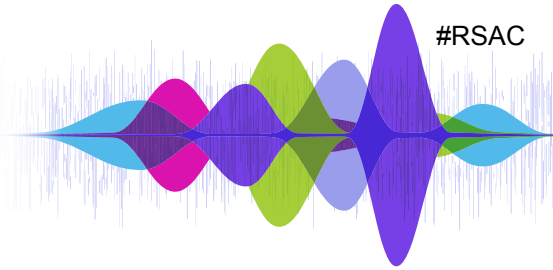


The AWS Console is Loud

0 Watchdog Insights

DATE	HOST	SERVICE	CONTENT
Mar 30 21:22:43.000		cloudtrail	{"eventID":"99a9ae3c-4a6b-4c37-9f0b-b78da73c3f3a","awsRegion":"us-east-1","evt":{"name":"DescribeAvailabilityZones"},"eventCategory":"Management","sessionCredentialFromConsole":"true","lev…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"52fa482b-c7e7-46ab-ba89-7a73cb9a2ede","awsRegion":"us-east-1","evt":{"name":"DescribePlacementGroups"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"e3534c91-d57f-4c54-badf-83d75b49d68c","awsRegion":"us-east-1","evt":{"name":"DescribeInstances"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":"Err…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"a351ae21-ce74-499e-b524-8b8a4c6ab1af","awsRegion":"us-east-1","evt":{"name":"DescribeVolumeStatus"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":"…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"3f02c891-aa60-4661-a6a4-a6adec1733ee","awsRegion":"us-east-1","evt":{"name":"DescribeVolumes"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":"Error…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"06eab072-df0d-4c3e-97ad-d07227bd88a7","awsRegion":"us-east-1","evt":{"name":"DescribeAccountAttributes"},"eventCategory":"Management","sessionCredentialFromConsole":"true","lev…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"898cdaf3-a4fb-4b1d-80ac-56dbbfc0e081","awsRegion":"us-east-1","evt":{"name":"DescribeSecurityGroups"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level"…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"a073fa30-ccbd-4b25-98da-b831bc5426b5","awsRegion":"us-east-1","evt":{"name":"DescribeHosts"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":"Error",…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"e35a2661-7190-49a1-bade-86c425b62052","awsRegion":"us-east-1","evt":{"name":"DescribeInstanceStatus"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level"…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"e481df35-dd75-433a-ad12-bb2307e6552b","awsRegion":"us-east-1","evt":{"name":"DescribeKeyPairs"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":"Erro…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"eaa1335a-1d82-4c76-86f4-c5129017faeb","awsRegion":"us-east-1","evt":{"name":"DescribeCapacityReservations"},"eventCategory":"Management","sessionCredentialFromConsole":"true","…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"9dc7b1dc-85a6-4ccb-9491-c4c8e2575178","awsRegion":"us-east-1","evt":{"name":"DescribeAddresses"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":"Err…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"27fe1876-a9a1-404d-9424-cfdbc9b7b3fd","awsRegion":"us-east-1","evt":{"name":"DescribeLaunchTemplates"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"4485f7ea-46b0-4fe9-8308-30f59a1ac1ca","awsRegion":"us-east-1","evt":{"name":"DescribeSnapshots"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":"Err…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"35eea513-7126-42c1-9c60-428c6961c732","awsRegion":"us-east-1","evt":{"name":"DescribeLoadBalancers"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":…
Mar 30 21:22:43.000		cloudtrail	{"eventID":"1e52bd54-07a6-4b0f-9880-6c6b5975f179","awsRegion":"us-east-1","evt":{"name":"DescribeLoadBalancers"},"eventCategory":"Management","sessionCredentialFromConsole":"true","level":…

sessionCredentialFromConsole



`sessionCredentialFromConsole`

String with a value of `true` or `false` that shows whether or not an event originated from an AWS Management Console session. This field is not shown unless the value is `true`, meaning that the client that was used to make the API call was either a proxy or an external client. If a proxy client was used, the `tlsDetails` event field is not shown.

Since: 1.08

Optional: True

Source: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html

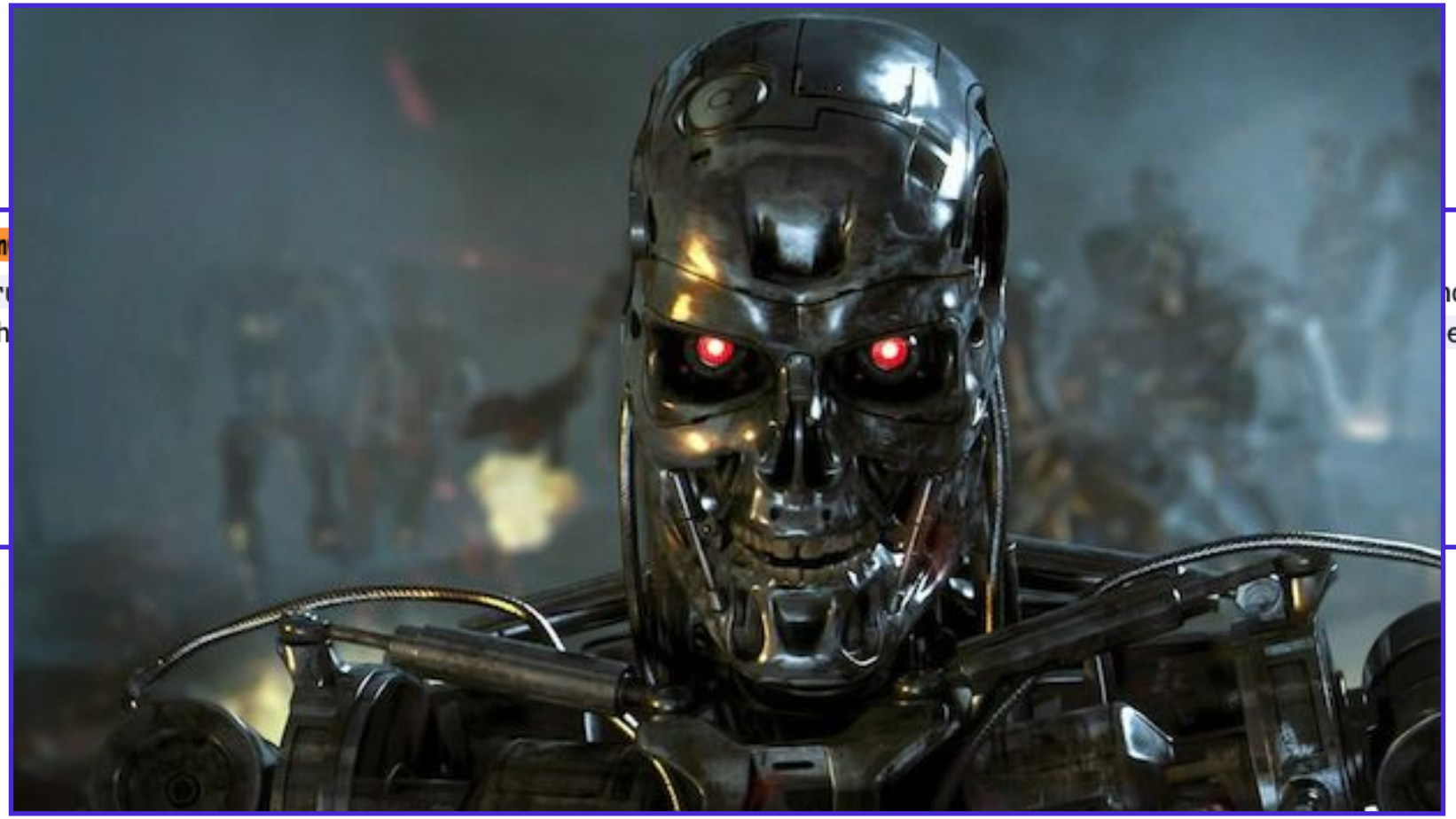
sessionCredentialFromConsole

sessionCredentialFrom

String with a value of tr
is true, meaning that th
shown.

Since: 1.08

Optional: True



not shown unless the value
etails event field is not

Source: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-event-reference-record-contents.html

Do you have IAM users?

- If your organization uses IAM users and Login Profiles, why are you using a signin token?

aws_consoler

- It’s also really easy to detect 😬

```
try:
    resp = sts.get_federation_token(
        Name="aws_consoler"
        PolicyArns=[
            {"arn": "arn:aws:iam::aws:policy/AdministratorAccess"}
        ])
    logger.debug("Federation session created, setting up session.")
```

RSAC™ | 2025 Conference

Lets talk about persistence

Persistence: Plenty of Options

- Create a new IAM user
- Create new keys for an existing user
- Create/Update login profile for an existing user
- Create a new IAM role
- Update trust policy on an existing role

Persistence: Plenty of Options

- **Create a new IAM user - 68%**
- Create new keys for an existing user - 11%
- Create/Update login profile for an existing user - 11%
- Create a new IAM role - 11%
- Update trust policy on an existing role - 0%

Persistence: Plenty of Options

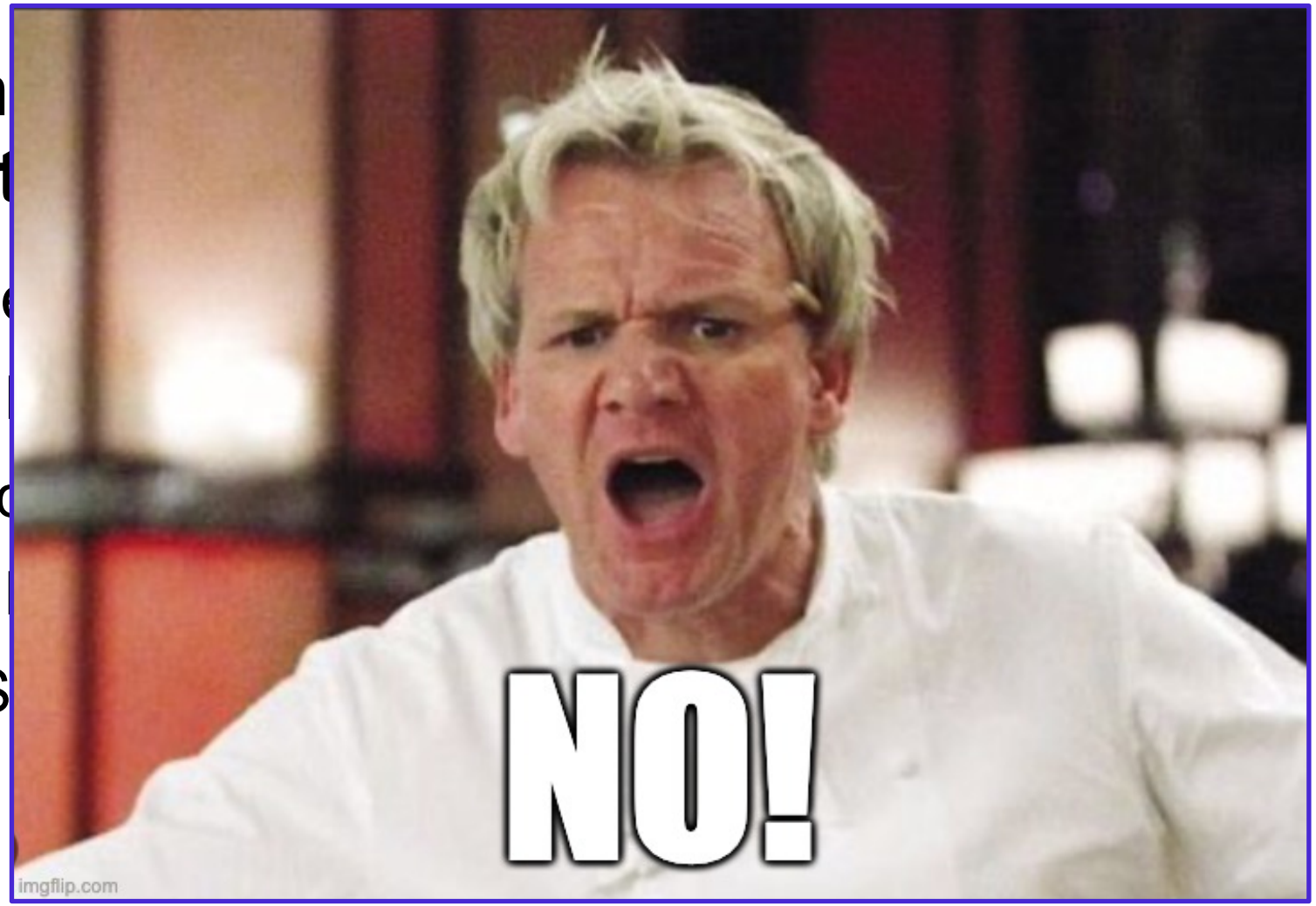
- **Create a new IAM user - 68%**
- Create new keys for an existing
- Create/Update login profile for a
- Create a new IAM role - 11%
- Update trust policy on an existin

Creating IAM User Blunders: You DON'T Need an Admin!

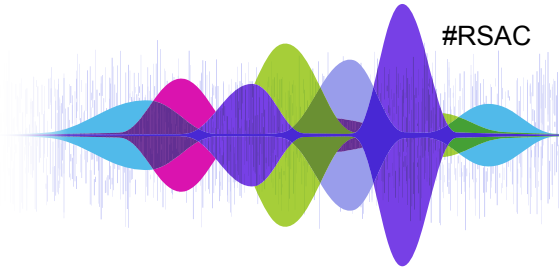
- **50% of new IAM users created were given the AdministratorAccess policy or equivalent!**
- Do you need access to:
  - Amazon Personalize?
  - AWS CodeStar?
  - Amazon Macie?
  - AWS FIS?

Creating IAM User Blunders: You DON'T Need an Admin!

- **50% of n**
  Administ
- Do you nee
  - Amazon
  - AWS Coc
  - Amazon
  - AWS FIS

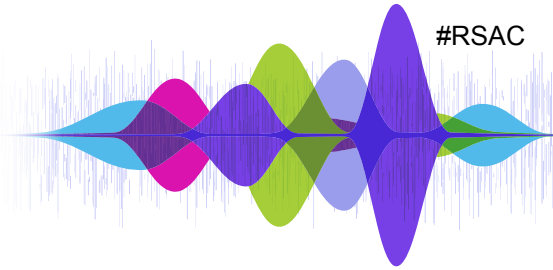


Creating IAM User Wins: Attackers Should Follow Least Privilege Too!



- When creating backdoor users, create simple, specifically privileged identities that give you the access you want.
- This creates less noise, and doesn't risk you getting caught by simple CNAPP and CSPM checks.

Creating IAM User Wins: Bonus Points! Why not obfuscate it?



- The IAM policy language is complicated….really complicated

Creating IAM User Wins: Bonus Points! Why not obfuscate it?

- The IAM policy language is complicated….really complicated
- **Let's abuse that!**

```
{
    "\u0053\u0074\u0061\u0074\u0065\u006d\u0065\u006e\u0074": [
        {
            "\u0045\u0066\u0066\u0065\u0063\u0074": "\u0041\u006c\u006c\u006f\u0077",
            "\u0041\u0063\u0074\u0069\u006f\u006e": [
                "iam:lIsT*",
                "iam:Create*",
                "iam:aTtAcHrOlE??????"
            ],
            "\u0052\u0065\u0073\u006f\u0075\u0072\u0063\u0065": [
                "*"
            ]
        }
    ],
    "\u0056\u0065\u0072\u0073\u0069\u006f\u006e": "\u0032\u0030\u0031\u0032\u002d\u0031\u0030\u002d\u0031\u0037"
}
```

Creating IAM User Wins: Bonus Points! Why not obfuscate it?

- The IAM policy language is complicated….really complicated
- **Let's abuse that!**
- Tons of ideas:
  - Unicode Encoding
  - Mixed casing
  - Wildcards (*, ?)
  - Not(Action, Resource)

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:lIsT*",
                "iam:Create*",
                "iam:aTtAcHrOlE??????"
            ],
            "Resource": [
                "*"
            ]
        }
    ],
    "Version": "2012-10-17"
}
```

Creating IAM User Wins: Bonus Points! Why not obfuscate it?

- The IAM policy language is complicated….really complicated
- **Let's abuse that!**
- Tons of ideas:
  - Unicode Encoding
  - Mixed casing
  - Wildcards (*, ?)
  - Not(Action, Resource)

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "NotAction": [
                "bugbust:GetJoinEventStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ],
    "Version": "2012-10-17"
}
```

Apply What You Have Learned Today

- Next week you should:
  - Create an inventory of active AWS access keys in your environment
- In the first three months following this presentation you should:
  - Delete those keys, and implement a plan (likely an SCP) to block the creation of future ones
- Within six months you should:
  - Ensure you have detections for suspicious User Agents in CloudTrail
  - Ensure you have detections for AWS principals with high numbers of access denied errors.
  - Ensure you have detections in place for IAM Users creating new IAM Users (With or without the AdministratorAccess policy 😊)

RSAC 2025 Conference

Many Voices.
One Community.

Thank you!

Find me on socials:

@Frichette_n

@frichetten.com

References (Page 1)

- Ransomware in the cloud
- Responding to an attack in AWS
- Decision---Commeasure-Pte-Ltd---15092021.pdf
- Incident report: From CLI to console, chasing an attacker in AWS
- Uber Security Update
- Anatomy of an Attack: Exposed keys to Crypto Mining
- Trouble in Paradise
- Tales from the cloud trenches: Amazon ECS is the new EC2 for crypto mining
- #AWS find of the week
- Kids' gaming website Animal Jam breached after miscreants spot private AWS key on pwned Slack channel
- SCARLETEEL 2.0: Fargate, Kubernetes, and Crypto
- M-Trends Report 2021
- The attack on ONUS – A real-life case of the Log4Shell vulnerability
- Unmasking GUI-Vil: Financially Motivated Cloud Threat Actor

References (Page 2)

- Decision---Sendtech-Pte-Ltd---220721.ashx
- Former Cisco engineer sentenced to prison for deleting 16k Webex accounts
- how to completely own an airline in 3 easy steps
- BrowserStack analysis: unpatched inactive machine compromised by shellshock vulnerability
- Compromised Cloud Compute Credentials: Case Studies From the Wild
- LUCR-3: Scattered Spider Getting SaaS-y in the Cloud
- Detecting AI resource-hijacking with Composite Alerts
- Tales from the cloud trenches: Unwanted visitor
- New Developments in LLM Hijacking Activity
- onelogin 2017 Security Incident
- Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments
- DXC spills AWS private keys on public GitHub
- Behind the scenes in the Expel SOC: Alert-to-fix in AWS
- Full Analysis of the PREMINT Attack Incident

References (Page 3)

- When a Zero Day and Access Keys Collide in the Cloud: Responding to the SugarCRM Zero-Day Vulnerability
- Clear and Uncommon Story about Overcoming Issues with AWS
- GotRoot! AWS root Account Takeover
- A Technical Analysis of the Capital One Cloud Misconfiguration Breach
- Chegg Complaint
- Tales from the cloud trenches: Raiding for AWS vaults, buckets and secrets
- Managed Detection & Response for AWS
- Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies
- SES-pionage
- The curious case of DangerDev@protonmail.me
- Tales from the cloud trenches: Using AWS CloudTrail to identify malicious activity and spot phishing campaigns
- Following attackers' (Cloud)trail in AWS: Methodology and findings in the wild
- Bling Libra's Tactical Evolution: The Threat Actor Group Behind ShinyHunters Ransomware
- JavaGhost's Persistent Phishing Attacks From the Cloud

References (Page 4)

- Safe{Wallet} incident
- New Phone, Who Dis? How Cloud Environments Are Exploited for Smishing Campaigns
- Incident 1 – Additional details of the attack Incident 2 – Additional details of the attack
- Navigating the Cloud: Exploring Lateral Movement Techniques
- Incident Report: TaskRouter JS SDK Security Incident - July 19, 2020
- LA Times homicide website throttles cryptojacking attack
- United States of America V Nickolas Sharp
- Imperva Security Update
- Compromised AWS Keys Abused in Codefinger Ransomware Attacks
- Otelier data breach exposes info, hotel reservations of millions
- pctattletale.com
- Why CISA is Warning CISOs About a Breach at Sisense
- Gov.uscourts.cand.375169.1.0_1.pdf
- Celeb Shout-Out App Cameo Exposes Private Videos and User Data

Leaked Access Keys

- With Admin access:
  - The curious case of DangerDev@protonmail.me
  - Incident report: From CLI to console, chasing an attacker in AWS
  - Anatomy of an Attack: Exposed keys to Crypto Mining - Stolen via vuln
  - Trouble in Paradise - Stolen via vuln (root)
  - Unmasking GUI-Vil: Financially Motivated Cloud Threat Actor
  - Decision---Sendtech-Pte-Ltd---220721.ashx
  - BrowserStack analysis: unpatched inactive machine compromised by shellshock vulnerability - Stolen via vuln
  - Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments - Found in a .env file
  - Behind the scenes in the Expel SOC: Alert-to-fix in AWS - root
  - GotRoot! AWS root Account Takeover - root
  - Imperva Security Update
  - Responding to an Attack in AWS (Leaked username and password)
  - Detecting AI resource-hijacking with Composite Alerts
  - Tales from the cloud trenches: Unwanted visitor
  - Clear and Uncommon Story about Overcoming Issues with AWS
  - pctattletale.com - root
- Otherwise:
  - Ransomware in the cloud
  - Tales from the cloud trenches: Amazon ECS is the new EC2 for crypto mining
  - #AWS find of the week
  - New Developments in LLM Hijacking Activity
  - onelogin 2017 Security Incident
  - DXC spills AWS private keys on public GitHub
  - Tales from the cloud trenches: Raiding for AWS vaults, buckets and secrets
  - Managed Detection & Response for AWS
  - SES-pionage
  - JavaGhost's Persistent Phishing Attacks From the Cloud
  - New Phone, Who Dis? How Cloud Environments Are Exploited for Smishing Campaigns
  - When a Zero Day and Access Keys Collide in the Cloud: Responding to the SugarCRM Zero-Day Vulnerability
  - Tales from the cloud trenches: Using AWS CloudTrail to identify malicious activity and spot phishing campaigns
  - Bling Libra's Tactical Evolution: The Threat Actor Group Behind ShinyHunters Ransomware
  - Compromised AWS Keys Abused in Codefinger Ransomware Attacks
  - Otelier data breach exposes info, hotel reservations of millions
  - Why CISA is Warning CISOs About a Breach at Sisense
  - how to completely own an airline in 3 easy steps
  - Decision---Commeasure-Pte-Ltd---15092021.pdf - Leaked in APK
  - Celeb Shout-Out App Cameo Exposes Private Videos and User Data
  - Kids' gaming website Animal Jam breached after miscreants spot private AWS key on pwned Slack channel

GetCallerIdentity

- Compromised Cloud Compute Credentials: Case Studies From the Wild
- Detecting AI resource-hijacking with Composite Alerts
- Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments
- When a Zero Day and Access Keys Collide in the Cloud: Responding to the SugarCRM Zero-Day Vulnerability
- Tales from the cloud trenches: Using AWS CloudTrail to identify malicious activity and spot phishing campaigns
- Following attackers' (Cloud)trail in AWS: Methodology and findings in the wild
- United States of America V Nickolas Sharp

Suspicious User Agent

- Anatomy of an Attack: Exposed keys to Crypto Mining (S3 Browser)
- Trouble in Paradise (S3 Browser)
- LUCR-3: Scattered Spider Getting SaaS-y in the Cloud (S3 Browser)
- #AWS find of the week - Kali user agent string
- Unmasking GUI-Vil: Financially Motivated Cloud Threat Actor (S3 Browser)
- Leaked Environment Variables Allow Large-Scale Extortion Operation in Cloud Environments (S3 Browser)
- Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies - Kali
- Bling Libra's Tactical Evolution: The Threat Actor Group Behind ShinyHunters Ransomware (S3 Browser)
- Safe{Wallet} incident - Kali

When a Zero Day and Access Keys Collide in the Cloud: Responding to the SugarCRM Zero-Day Vulnerability - Scout Suite

Console Access

- The curious case of DangerDev@protonmail.me
- Responding to an attack in AWS
- Incident report: From CLI to console, chasing an attacker in AWS
- Anatomy of an Attack: Exposed keys to Crypto Mining
- Tales from the cloud trenches: Amazon ECS is the new EC2 for crypto mining
- Unmasking GUI-Vil: Financially Motivated Cloud Threat Actor
- LUCR-3: Scattered Spider Getting SaaS-y in the Cloud
- Detecting AI resource-hijacking with Composite Alerts
- Tales from the cloud trenches: Unwanted visitor
- Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies
- GotRoot! AWS root Account Takeover
- JavaGhost's Persistent Phishing Attacks From the Cloud

Creating an IAM User

- With Admin access:
  - The curious case of DangerDev@protonmail.me
  - Responding to an attack in AWS
  - Incident report: From CLI to console, chasing an attacker in AWS
  - Anatomy of an Attack: Exposed keys to Crypto Mining
  - BrowserStack analysis: unpatched inactive machine compromised by shellshock vulnerability
  - Tales from the cloud trenches: Unwanted visitor
  - Tales from the cloud trenches: Amazon ECS is the new EC2 for crypto mining
  - JavaGhost's Persistent Phishing Attacks From the Cloud
- Otherwise:
  - Trouble in Paradise
  - #AWS find of the week (failed)
  - SCARLETEEL 2.0: Fargate, Kubernetes, and Crypto
  - M-Trends Report 2021
  - Unmasking GUI-Vil: Financially Motivated Cloud Threat Actor
  - Compromised Cloud Compute Credentials: Case Studies From the Wild (failed)
  - LUCR-3: Scattered Spider Getting SaaS-y in the Cloud
  - Detecting AI resource-hijacking with Composite Alerts
  - New Developments in LLM Hijacking Activity
  - Ransomware in the cloud (failed)
  - Following attackers' (Cloud)trail in AWS: Methodology and findings in the wild